



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/841,689 | 04/23/2001 | Stephen Sorkin | RECOP008 | 4377 |

21912 7590 05/13/2004

VAN PELT & YI LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

| |
|----------|
| EXAMINER |
|----------|

BAUM, RONALD

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2136

DATE MAILED: 05/13/2004

10

Please find below and/or attached an Office communication concerning this application or proceeding.

SC

Office Action Summary

Application No.

09/841,689

Applicant(s)

SORKIN ET AL.

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 3,4,6,7,9,13-15,20,29,30,32,33,35 and 37-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 3,4,6,7,9,13-15,20,29,30,32,33,35 and 37-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

Art Unit: 2136

DETAILED ACTION

1. The previous office action (2/3/2004) is withdrawn.
2. Claims 3,4,6,7,9,13-15,20,29,30,32,33,35,37-41 are pending for examination.
3. Claims 3,4,6,7,9,13-15,20,29,30,32,33,35,37-41 are rejected.

Specification

The disclosure objection concerned with improper reference to documents being incomplete without more specific identification (i.e., actual US patent applications numbers) is withdrawn.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

The term "possible" in claims 3,4,6,7,9,13-15,20,29,30,32,33,35,37-41 is a relative term which renders the claim indefinite. The term "possible" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. A "possible sgid" or "possible suid" exploit could encompass no exploit (i.e., nothing is searched for in the query), to some specific entries that makes up the method query search criteria. For the purpose of applying art, the term will be assumed to refer to criteria (i.e., event lines sequences) that affirm the existence of a suid / sgid exploit.

The phrase "method further" in claims 38,39 is applied to a system / apparatus claim which renders the claim indefinite. For the purpose of applying art, the phrase will be assumed to be 'pattern searched comprises aggregated...".

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 3,4,6,7,9,13-15,20,29,30,32,33,35,37-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Crosbie et al, "IDIOT - Users Guide", Technical Report TR-96-050, Perdue University, September 4, 1996.

5. As per claim 3; "A method for analyzing a logfile produced by a computer network security system [entire document, as per description in Chapter 5] comprising: providing a regular expression query associated with a pattern to be searched for in the logfile [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the (i.e., C++) pattern programs).]; and using the query to search for the pattern in the logfile [entire document, as per description in Chapter 4 (i.e., audit trail)]; wherein the pattern is associated with a possible *sgid* exploit and using the query to search for the pattern includes searching for entries showing that a process has been started with effective group ID equal to zero [entire document, as per

Art Unit: 2136

description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of *sgid* term is taught (pages 6,25,30,50-54,60), and further, the effective group ID equal to zero is the same as granted super-user or root permission status).].”;

And further as per claim 29; “A system [This claim is the apparatus of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above] for analyzing a logfile produced by a computer network security system comprising: a storage including a regular expression query associated with a pattern to be searched for in the logfile; and a processor configured to use the query to search for the pattern in the logfile; wherein the pattern is associated with a possible *sgid* exploit and the processor is further configured to search for entries showing that a process has been started with effective group ID equal to zero.”;

And further as per claim 35; “A computer program product [This claim is the embodied software on computer readable media of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above] for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for providing a regular expression query associated with a pattern to be searched for in the logfile; and using the query to search for the pattern in the logfile; wherein the pattern is associated with a possible *sgid* exploit and using the query to search for the pattern includes searching for entries showing that a process has been started with effective group ID equal to zero.”.

Art Unit: 2136

6. As per claim 6; “A method for analyzing a logfile produced by a computer network security system [entire document, as per description in Chapter 5] comprising: providing a regular expression query associated with a pattern to be searched for in the logfile [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the (i.e., C++) pattern programs).]; and using the query to search for the pattern in the logfile [entire document, as per description in Chapter 4 (i.e., audit trail)]; wherein the pattern is associated with a possible *suid* exploit and using the query to search for the pattern includes searching for entries showing that a process has been started with effective user ID equal to zero [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of *suid* term is taught (pages 2-14,16-18,21,23-25,27,29-37,39,50-55,59,60), and further, the effective user ID equal to zero is the same as granted super-user or root permission status).].”;

And further as per claim 32; “A system [This claim is the apparatus of the method claim 6, and is rejected for the same reasons provided for the claim 6 rejection above] for analyzing a logfile produced by a computer network security system comprising: a storage including a regular expression query associated with a pattern to be searched for in the logfile; and a processor configured to use the query to search for the pattern in the logfile; wherein the pattern is associated with a possible *suid* exploit and the processor is further configured to search for entries showing that a process has been started with effective user ID equal to zero.”;

And further as per claim 37; “A computer program product [This claim is the embodied software on computer readable media of the method claim 6, and is rejected for the same reasons provided for the claim 6 rejection above] for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for providing a regular expression query associated with a pattern to be searched for in the logfile; and using the query to search for the pattern in the logfile; wherein the pattern is associated with a possible *suid* exploit and using the query to search for the pattern includes searching for entries showing that a process has been started with effective user ID equal to zero.”.

7. Claim 4 ***additionally recites*** the limitations that; “The method as recited in claim 3, wherein using the query to search for the pattern further includes storing a process ID of the process, and searching for processes with a parent process ID equal to the stored process ID [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of the term PID (pages 10,13,15,17-19,21,22,27-29,31-34,37-40,44,50-56,59) is taught.].”;

And further as per claim 30; “The system as recited in claim 29 [This claim is the system of the method claim 4], wherein the processor is further configured to store a process ID of the process, and search for processes with a parent process ID equal to the stored process ID.”;

8. Claim 7 ***additionally recites*** the limitations that; “The method as recited in claim 6, wherein using the query to search for the pattern further includes storing a process ID of the process, and searching for processes with a parent process ID equal to the stored process ID

Art Unit: 2136

[entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of the term PID (pages 10,13,15,17-19,21,22,27-29,31-34,37-40,44,50-56,59) is taught.].”;

And further as per claim 33; “The system as recited in claim 32 [This claim is the system of the method claim 7], wherein the processor is further configured to store a process ID of the process, and search for processes with a parent process ID equal to the stored process ID.”.

9. As per claim 9; “A method for analyzing a logfile produced by a computer network security system [entire document, as per description in Chapter 5] comprising: providing a regular expression query associated with a pattern to be searched for in the logfile [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the (i.e., C++) pattern programs).]; and using the query to search for the pattern in the logfile [entire document, as per description in Chapter 4 (i.e., audit trail)]; wherein the pattern is associated with a possible *sgid* exploit, the pattern is associated with processes spawned by a shell, and using the query to search for the pattern includes searching for entries showing that the shell has started a process, storing a process ID of the process, and searching for entries showing processes with parent process equal to the stored process ID [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of the *sgid* (pages 6,25,30,50-54,60) and PID (pages 10,13,15,17-19,21,22,27-29,31-34,37-40,44,50-56,59) terms is taught.].”.

Art Unit: 2136

10. As per claim 13; “A method for analyzing a logfile produced by a computer network security system [entire document, as per description in Chapter 5] comprising: providing a regular expression query associated with a pattern to be searched for in the logfile [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the (i.e., C++) pattern programs).]; and using the query to search for the pattern in the logfile [entire document, as per description in Chapter 4 (i.e., audit trail)]; wherein the pattern is associated with a possible *sgid* exploit, the pattern is associated with screen output characters, and the method further comprises aggregating the screen output characters found in the logfile [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of the ‘pattern is associated with screen output characters, and the method further comprises aggregating the screen output characters found in the logfile’ phrase is interpreted by the examiner to refer to the rendered on the screen (i.e., string, ASCII character type text data) form of data (i.e., page 45, 46).].”;

And further as per claim 38; “A system [This claim is the apparatus of the method claim 13, and is rejected for the same reasons provided for the claim 13 rejection above] for analyzing a logfile produced by a computer network security system comprising: a storage including a regular expression query associated with a pattern to be searched for in the logfile; and a processor configured to use the query to search for the pattern in the logfile; wherein the pattern is associated with a possible *sgid* exploit, the pattern is associated with screen output characters, and the method further comprises aggregating the screen output characters found in the logfile.”;

And further as per claim 39; “A computer program product [This claim is the embodied software on computer readable media of the method claim 13, and is rejected for the same reasons provided for the claim 13 rejection above] for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for providing a regular expression query associated with a pattern to be searched for in the logfile; and using the query to search for the pattern in the logfile; wherein the pattern is associated with a possible *sgid* exploit, the pattern is associated with screen output characters, and the method further comprises aggregating the screen output characters found in the logfile.”.

11. Claim 14 *additionally recites* the limitations that; “The method as recited in claim 13, wherein the found screen output characters are aggregated upon finding a screen output character representing a newline character [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of the ‘found screen output characters are aggregated upon finding a screen output character representing a newline character’ phrase is interpreted by the examiner to refer to the rendered on the screen (i.e., string, ASCII character type text data) form of data that is ‘event line terminated’ via a LF and/or CR character which would be inherent in the IDIOT system because of the use of UNIX based environment for the logfile (i.e., page 45, 46).].”.

12. Claim 15 *additionally recites* the limitations that; “The method as recited in claim 14, further comprising presenting the aggregated keystrokes to a second user character [entire

Art Unit: 2136

document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of the 'found screen output characters are aggregated upon finding a screen output character representing a newline character' phrase is interpreted by the examiner to refer to the rendered on the screen (i.e., string, ASCII character type text data) form of data that is 'event line terminated' via a LF and/or CR character which would be inherent in the IDIOT system because of the use of UNIX based environment for the logfile (i.e., page 45, 46). Further, since the system is used in a clearly multi-user environment, a 'second' user event(s) dealing with access to monitored files would clearly be part of the logfile.].”.

13. As per claim 20; “A method for analyzing a logfile produced by a computer network security system [entire document, as per description in Chapter 5] comprising: providing a regular expression query associated with a pattern to be searched for in the logfile [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the (i.e., C++) pattern programs).]; and using the query to search for the pattern in the logfile, including by searching for entries showing a monitored file has been accessed, indicating to a second user a process ID of a process that accessed the monitored file; and automatically searching for the process ID in the logfile; wherein the pattern is associated with a possible *sgid* exploit [entire document, as per description in Chapter 4 (i.e., the compiled, linked and executed pattern applied to the audit trail, whereas the regular expression query associated with a pattern is the pattern programs (i.e., pages 2,3,6,10-13,16,29-35,59) whereas the explicit and implicit use of the *sgid*

Art Unit: 2136

(pages 6,25,30,50-54,60) and PID (pages 10,13,15,17-19,21,22,27-29,31-34,37-40,44,50-56,59)

terms is taught, and further that file access (of monitored files) by virtue of the read / write / execute file permissions dealing with file access events audited via pattern software creation would clearly be inherent. Further, since the system is used in a clearly multi-user environment, a 'second' user event(s) dealing with access to monitored files would clearly be part of the logfile.].”;

And further as per claim 40; “A system [This claim is the apparatus of the method claim 20, and is rejected for the same reasons provided for the claim 20 rejection above] for analyzing a logfile produced by a computer network security system comprising: a storage including a regular expression query associated with a pattern to be searched for in the logfile; and a processor configured to use the query to search for the pattern in the logfile, including by searching for entries showing a monitored file has been accessed, indicating to a second user a process ID of a process that accessed the monitored file; and automatically searching for the process ID in the logfile; wherein the pattern is associated with a possible *sgid* exploit.”;

And further as per claim 41; “A computer program product [This claim is the embodied software on computer readable media of the method claim 20, and is rejected for the same reasons provided for the claim 20 rejection above] for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for providing a regular expression query associated with a pattern to be searched for in the logfile; using the query to search for the pattern in the logfile, including by searching for entries showing a monitored file has been accessed, indicating to a second user a process ID of a process that accessed the monitored file; and automatically

Art Unit: 2136

searching for the process ID in the logfile; wherein the pattern is associated with a possible *sgid* exploit.”.


Conclusion

14. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu, can be reached at (703) 305-4393. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100